Introduction to Cybersecurity

Project documentation

Mahmud Yusifli - 12341180

25.06.2024

- Python version: 3.11.7 under Windows 10
- Chosen MPC function: Maximum of two sets of values
- Used repository: https://github.com/ojroques/garbled-circuit

Requirements:

pip3 install --user pyzmq cryptography sympy

to run execute command: python ./main.py bob

- party could be “bob” or “alice”

Introduction

The main aim of the project is to implement a computation of maximal value of two set of numbers. Main task was to prepare program which allows communication and secure computation of data between Alice and Bob. It is required that data was to be at least 4 bits of size. Unfortunately, there were still some issues with my code. However, I gained sufficient information about MPC and Yao protocol. Although, the project did not achieve all required rules due to technical difficulties and encountered challenges, I gained significant learning outcomes and valuable information.

I appreciate your understanding of the complexities and challenges that could not be resolved. The lessons learned from these obstacles will undoubtedly contribute to future success in similar endeavors.

2. Differences from base repository/used methods

This section contains the differences between the given repository and my implementation. All file names discussed and explained separately in this section.

-Util.py:

nothing changed

-Garbleryao.py:

YaoGarbler moved here. LocalTest class also movd here from main,py

-Alice.py:

new: compute response, and alice class

-Bob.py:

new: compute response, and bob class

-Main.py:

This file is responsible for the execution of the program. It contains the argument parser.

-Yao.py:

no changes made. All the code is original code.